SIGNATURE DYNAMICS

ELECTRONIC SIGNING POLICY

for electronic signature use

version as of April 25, 2001
the current version may be found at
http://www.sos.state.az.us/pa/default.htm

State of Arizona
Policy Authority
Office of the Secretary of State

ARIZONA ELECTRONIC SIGNATURE INFRASTRUCTURE (AESI)
Signature Dynamics Electronic Signatures (SDES)
VERSION 1.00
April 2002

TABLE OF CONTENTS

1 Introduction

This Electronic Signing Policy[1] defines Arizona's Signature Dynamics Electronic Signing Policy – Basic Assurance Level. This Policy is for use in the Signature Dynamics portion of the State of Arizona's Electronic Signature Infrastructure (AESI)[1] as defined and managed by Arizona's Policy Authority (PA).

This document uses several technical concepts associated with Signature Dynamics and electronic signing technologies. To become familiar with the terminology used, we strongly recommend that you read the Electronic and Digital Signature Definitions and Acronyms document before reading this one and then refer to it as needed while reading this.

The security mechanisms provided by the AESI are not intended to be used alone for the protection of classified or sensitive information.

2 Policy Specification

2.1 Overview

This Electronic Signing Policy is intended for use by State of Arizona agencies, boards, commissions and their electronic signing partners in Signature Dynamic based electronic signature activity.

Signature Dynamics allows individuals to create their own biometric based electronic signature and have it recognized as valid by other parties. Signature Dynamics electronic signatures can be created by various biometric based technologies. There is neither a generally accepted technical standard for these biometric based technologies nor a generally accepted method to evaluate the security of the business process employed to use the technology. The particular business process scope and minimum technical requirements of this Electronic Signing Policy are specified in Section 5 – *Operational Requirements.*

Communities of interest (ESI's), determine what level of trust (basic, medium, and high) is appropriate for their needs (see Section 4.8.1). This Signature Dynamics Electronic Signing Policy is for a Basic assurance level only. Applications requiring higher assurance must incorporate a technology approved for those higher levels of trust. This does not preclude using Signature Dynamic signing technologies in circumstances requiring higher levels of trust. It merely requires additional technology to provide the additional trust needed. If an ESI finds a particular Electronic Signing Policy (or Policies) does not provide the exact degree of trust needed, it should accept and use the Policy combination that provides the closest *less* restrictive level of trust and then incorporate additional requirements necessary into a binding agreement among the

[1] taking liberties with IETF's conception of PKI (Public Key Infrastructure), AESI is Arizona's collections (note plural) of electronic signing mechanisms and the entities and tools that support and provide the means to validly use these mechanisms as signatures. The concept of "Electronic Signing Policy" is also extended from PKI Certificate Policy concept to being any policy document governing an electronic signing technology. Each technical signing process will have one or more "Electronic Signing Policies" defining the framework for the use of that technology for electronic signatures by and with Arizona state agencies.

parties. They may not reduce or otherwise undermine the terms and conditions of this Electronic Signing Policy or any combination of Electronic Signing Policies. Relying Parties rely on the Electronic Signing Policies being fully enforceable.

The electronic signature policies in this Electronic Signing Policy are for management and use of Signature Dynamic (biometric) electronic signature processes.

A signing using an electronic signature process approved by any of Arizona Electronic Signing Policies does not imply that the Signer has any authority to conduct business transactions on behalf of an organization.

Any required signing tool or signer registration repository's compliance with this Electronic Signing Policy will be governed by the laws of the State of Arizona and any applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Electronic Signing Policy.

The Signature Dynamic Tool Provider compliance with this Electronic Signing Policy is governed by the laws of the State of Arizona and applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Electronic Signing Policy.

Any required Registration Authority's[2] compliance with this Electronic Signing Policy is to be governed by the laws of the State of Arizona and applicable Federal and local law concerning enforceability, construction, interpretation and validity of this Electronic Signing Policy.

The State of Arizona will not enter into a cross certification or reciprocity agreement with another Signature Dynamic electronic signature community without the approval of the Policy Authority.

2.2 Policy overview

The Policy Object Identifier Designation for this Policy is registered under the Policy Authority arc { joint-iso-ccitt (2) country (16) us (840) state (3) AZ (04) EB (01) Secretary of State (002) DO (02) Policy Authority (999)} as OO (00) id-AESIsigdyn-certpcy-sign-1 (004). This policy is designed for use in certain situations and it identifies specific roles needed for effectiveness in those situations. Signers, Relying Parties and parties assuming delegated roles all have specific obligations outlined in this policy.

The Signers and Relying Parties must agree on a method (a technology and its related signing processes) to securely sign and then securely store the signed electronic records.

The Signers and Relying Parties must agree on a method to identify Signers and link the electronic signature to them. The identification method is managed by the party known as

[2] A Registration Authority is another PKI term used in a broader sense here to mean the party responsible for linking the Signer to the Signature (who's signature is it?). The role and its responsibilities will be very much defined by the community's signing requirements and the process actually deployed to meet that need.

a Registration Authority. Any of the parties may be the Registration Authority or a mutually agreed third party may do so. The party acting as the Registration Authority must contractually agree to comply with this Electronic Signing Policy and any other agreement between it and the Signers and Relying Parties.

This Electronic Signing Policy is appropriate to sign documents that, if compromised, could cause minimal injury to State of Arizona interests unless there is an explicit agreement by the agency (or agencies) participating in the ESI to alter this limitation.

The State of Arizona disclaims all liability for any use of this certificate type other than uses permitted by this document. The State of Arizona limits its liability for permitted uses to $0 per instance of use unless there is an explicit agreement by the agency (or agencies) participating in the ESI to extend that limit.

Any disputes concerning signing process or records management under this policy are to be resolved by the Parties concerned using an appropriate dispute settlement mechanism (i.e. through negotiation, mediation or arbitration).

Identification and authentication will be in the manner set out in this policy.

2.3 Identification alphanumeric OID

id-AESIsigdyn-certpcy-digitalSignature-basicAssurance ::= { id-AESIsigdyn-certpcy-sign-4 }

Certificate Types (levels of signing process trust)

The Basic certificate type and OID will be recognized for use within the ESI established by this Electronic Signing Policy. The ESI electronic signature level (Basic, Medium, High) is determined from the matrix of trust levels in section 2.4.8.1. The certificate types used by the state of Arizona — Basic, Medium and High — vary depending on the method of identifying the Signer, the method for linking the Signer to the Certificate and the processes for assuring the Integrity of the Record [see 2.4.8.1]. The Certificate assigned should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, and Signature Linkage to the Integrity of the Record. Each level of Certificate subsumes the level(s) below it.

All Agreements and documents linking a Signature Dynamic signing process to this Electronic Signing Policy will contain OID:

- Basic Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.004.01.01

Any Signature Dynamic signing process needing a higher level of trust must combine the Signature Dynamic signing process with another signing technology that provides the needed level of trust within the framework of signing processes approved by the PA.

2.4 Community and applicability

The State of Arizona's Electronic Signature Infrastructure (AESI), and its Signature Dynamic infrastructure, are managed by the Office of the Secretary of State which is the Policy Authority (PA) in accordance with appropriate Statute and Administrative Rules.

This Policy describes a Signature Dynamic infrastructure within AESI. This Signature Dynamic infrastructure is used by bounded communities of interest. A bounded Signature Dynamic community of interest is described in this document as an Electronic Signature Infrastructure (ESI). The ESI is designed to enable the use of electronic signatures as the equivalent of handwritten signatures. This requires a range authenticity and verification protections similar to a handwritten signature on a physical document. It also requires, given its nature, additional protections to prevent repudiation.

An ESI community is comprised of Signers and Relying Parties who have mutually agreed to participate in this community and any parties that they have agreed to delegate specific roles to.

2.4.1 Description of Signature Dynamic infrastructure

Any Signature Dynamic electronic signing requires the mutual agreement of parties to employ an approved Signature Dynamic signing process to sign in an agreed upon fashion. This requires agreement on:

1. How the Signer is authenticated as the party they represent themselves to be,
2. Who provides the Signature Dynamic signing process tools (one or more of the parties or an agreed on third party) and agreement that the method used assures the Signer has sole possession of the means of creating their electronic signature,
3. How the electronic signature validity is ascertained by any legally interested party,
4. How the record integrity is be ascertained and how that integrity is linked to the Signer's electronic signature with any legally interested party able to verify that integrity and link.
5. Agreement that the reception of a record linked to a valid electronic signature and with proof of record integrity completes a legally binding record signing by the Signer.

This Policy is binding on each party participating in electronic signing processes that identify this Policy, and governs each party's performance with respect to all signings and acceptance of signatures done within that Electronic Signing Policy conforming electronic signing process.

All Signers using Signature Dynamics based signatures shall use signing tools issued in accordance with this Electronic Signing Policy. Should a state Agency use a contractor to provide signing or signed record storage services, the Agency remains responsible and accountable for the operation of its contractors.

2.4.2 Registration Authorities

By its nature Signature Dynamics is designed to work without a Registration Authority. However, the Signers and Relying Parties may have need to agree to have a Registration Authority (RA) perform Signer identification and signature verification services. And, if

so agreed, who might perform the role and functions of the Registration Authority. They may subcontract Registration Authority functions to a third party who agrees to be bound by this Policy, but the Signers and Relying Parties remain responsible for the performance of those services in accordance with this Policy and the requirements of their AESI Contract.

2.4.3 Signing Tool Manufacturing Authorities

The ESI's Signers and Relying Parties must agree on who provides the Signature Dynamic signing tools (one or more of the parties or an agreed on third party) and agree that the signing tool and related methods assure the Signer has sole possession of the signing tool and that any resulting signature is uniquely linked to the Signer. The Signers and Relying Parties remain responsible for the performance of any subcontracted services in accordance with this Policy and the requirements of their AESI Contract.

2.4.4 Local Registration Authorities (LRAs)

If there is a Registration Authority needed, the Signers and Relying Parties may determine that a Registration Authority function should be delegated to Local Registration Authority. Delegation of the RA's Signer identification function is typical. An LRA operating under this Electronic Signing Policy is responsible for all duties assigned to it by the Signers and Relying Parties or their RA subcontractor(s).

An LRA may perform RA duties providing that in doing so it satisfies all the requirements of this Electronic Signing Policy.

2.4.5 Signers

Signature Dynamic signing tools that reference this Policy may be issued to the following classes of Signers:

- individuals (unaffiliated)
- individuals associated with a sponsor recognized by the ESI ("affiliated individuals"), provided the sponsor is a qualified Signer within the ESI in accordance with this Policy.
- organizations that qualify as legal entities if responsibility and accountability are attributable to a designated living agent for the organization.
- government agencies if responsibility and accountability are attributable to a designated living agent for the agency.

2.4.6 Relying parties

This Policy benefits the following persons who may rely on Certificates issued to others that reference this Policy (Qualified Relying Parties):

- State government agencies that specify this Policy by regulation
- Federal and other government agencies that specify this Policy by regulation
- Businesses that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.
- Individuals that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.

2.4.7 Policy applicability

This Electronic Signing Policy is suitable to assure transaction integrity and authenticity within the originator's approval limits and where falsification of the transaction would cause only minor financial loss or require only administrative action for correction.

2.4.8 Approved and prohibited applications

2.4.8.1 Electronic Signature Framework of Trust

Each signing community will need to evaluate the levels of risk associated with their signing processes and associate those risks to a framework that defines three levels of trust in evaluating signed electronic record authenticity, reliability, and integrity. Each trust level should be related to the potential risk involved in and levels of security for the highest risk type of transaction. The defined trust levels are:

- **Basic** - This level provides a basic level of assurance relevant to transactions where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

- **Medium** - This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

- **High** - This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

This policy will identify appropriate implementations for basic, medium, and high trust levels as far as how the:

- Signer identification.
- Signer link to signature.
- Signature link to record integrity.

2.4.8.1.1 Signer Identification

Signer identification refers to the method by which an individual is identified and authorized to use a particular electronic signature method. Signer identification is independent of the signature or records creation technology being employed. However, it is critical to the level of trust that can be attributed to a signed record because the more robust or stringent the method of identification and authorization the more assurance that the signature has been authorized for use by the person who he or she purports to be. The identification and authentication methods for each level of trust are displayed in the table below.

Basic	• A government entity, its agent or an appropriate individual licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing an electronic signature compared the identity of the individual with two pieces of identification (copies or originals). At least one of these must be a government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • A sponsoring government entity or its agent has compared trusted information in a data base with user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or • By attestation of a supervisor, or administrative or information security officer, or an individual certified or licensed by a government entity as being authorized to confirm identities (e.g., notary) who uses a stamp, seal or other mechanism to authenticate their identity confirmation
Medium	• A government entity, its agent or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing compared the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • A sponsoring government entity or its agent has previously established the

	identity of an individual using a process that satisfies the above requirements and there have been no changes in the information presented.
High	• A government entity, its agent, or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities, in the presence of the individual for the purposes of authorizing or issuing a signature, compares the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government identification containing a photograph (e.g., driver's license, non-driver identification, passport).

Along with the above identification requirements, the originating government entity or its agent must keep a record of the type and details of identification used and on request make it available to the state entity receiving the signed record for that signed record to be accepted at the purported trust level.

2.4.8.1.2 Signer Linkage to Signature

Signer linkage to signature refers to the policy, process and procedures establishing a link between the signer and the information and method used to sign. This linkage has two dimensions.

1. The first dimension is the way by which the unique signature characteristics are linked to the signer. This linkage can be achieved through one thing or by a combination of things only the individual:

   - ***Knows*** (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key);
   - ***Possesses*** (a token -- e.g., an ATM card or a smart card); or
   - ***Is*** (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, retinal scan or a fingerprint).

2. The second dimension is trust level. Trust level is closely related to the specific signing method (e.g., shared secrets, biometric, cryptographic keys).

   The level of trust of an electronically signed record is in part a function of how convinced the receiving government is that the information used to sign has remained

in the sole possession of the individual authorized to use it. In developing the levels of trust for this component of the policy it is assumed that there will be multiple ways to meet the requirements of each level and that multiple methods could theoretically meet the requirements of the same level.

The methods for linking signers to signing information or electronic signatures for each level of trust are displayed in the table below.

Basic	• Two shared secrets (e.g., pin, password) where a governmental body has assigned at least one secret and the signer has been provided with and has conformed to appropriate security standards as far as protecting the shared secrets. • A shared secret[3] and a private cryptographic key or biometric information in which the cryptographic key cannot be accessed without the shared secret. "Private" in this sense means in the sole possession of the signer.
Medium	• Three shared secrets in which one has been assigned by a governmental body and one consists of private information that only the signer would know (e.g., income tax information), and the third could be selected by the signer. • A shared secret and a private cryptographic key or biometric stored in a secure software token on a secure computer.
High	• A shared secret and a cryptographic key or biometric stored on a hardware token where the key or biometric cannot be accessed without the shared secret and the shared secret is only known by the signed and the hardware token. • A biometric where the signer needs to be present to sign.

Along with the above identification requirements, the originating government entity or its agent must keep a record of the methods and approaches used to link a signer to signature information.

[3] Appropriate Signature Dynamics technologies will have a mechanism for signature analysis and verification. This mechanism, with appropriate security, serves as a shared secret.

2.4.8.1.3 Signature Linkage to the Integrity of the Record

This element of trust has two components.

1. An electronic signature must be linked to the record to which it is affixed or associated. E-signatures can be linked to an e-record in many different ways. The e-signature can become part of the record's data structure or imbedded as a data object within the document. The e-signature can also be stored in a different location but logically linked to the e-record. However, a government agency must manage the e-record and electronic signature as a unit and ensure that the link between them is maintained for the record's legal minimum retention period.

2. There must be some method to ensure that the signature is linked to the record content that the signer intended to sign in such a manner that any change to the record since the record was signed is detectable and invalidates the signature.

This signature linkage to the integrity of the record is achieved by the system that collectively manages the e-record and the associated signature. In such a case, trust is a function of the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified and the system's ability to detect that such has occurred. However, transferring agencies also need to use a transmission method to ensure that the integrity of the electronically signed record is not compromised. Linkage can also be created using technologies in which the signature and record exist as a unified object in which validation of the signature itself provides assurances that the record and signature have not been tampered with or modified. Technologies that use cryptography and hashing techniques can achieve this outcome.

The methods for linking an electronic signature to the integrity of the record for each level of trust are displayed in the table below.

Basic	• Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link.[4] Transferring agencies have mutually agreed to a secure method for: transferring the

[4] NIST SP 800-14***Generally Accepted Principles and Practices for Securing Information Technology Systems*** will serve as a general guideline for generally accepted system security practices.

	electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link.
Medium	• An outside entity or auditor has certified that the system used to capture and manage the electronically signed record reasonably ensures, through compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to: a secure method for transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link. • Self-certification that system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link Transferring agencies have mutually agreed to secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic method (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record.
High	• An outside entity or auditor has certified that the system used to capture and manage electronically signed record reasonably ensures, through compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually

	agreed to: a secure method for transferring the electronically signed record and secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic methods (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record. • Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to a secure method for transferring the electronically signed record and to the use of a cryptographic method with hashing techniques to ensure record integrity and the link between the record and the signature (e.g., PKI)

2.4.8.2 Approved Applications

Signature Dynamics signing processes referencing this Policy may be used for any purpose authorized by regulations adopted by Qualified Relying Parties, except to the extent specifically prohibited by agreements among the ESI Signers and Relying Parties.

The ESI electronic signature level (Basic, Medium, High) is determined from the matrix of trust levels. The signing method used should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, Signature Linkage to the Integrity of the Record.

This Signature Dynamics Electronic Signing Policy is only valid for Basic electronic signatures. Medium or High trust level electronic signing processes may only use Signature Dynamics when combined with another signing technology that provides the additional trust level needed.

2.4.8.3 Prohibited Applications

Signing processes that reference this Policy may not be used for any application requiring fail-safe performance such as the operation of nuclear power facilities,

air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or environmental damage.

Signing processes referencing this Policy should not be used for transactions where the per use value exceeds $5,000.00 without the explicit agreement among the parties.

2.4.9 Contact details

This Policy is administered by the Policy Authority:

State of Arizona
Office of the Secretary of State
1700 W. Washington #7
Phoenix, Arizona 85007

2.4.9.1 Policy Authority contact person:

Russ Savage
Phone number: 602.542.2022
E-mail address: pa@mail.sosaz.com

2.4.9.2 Contact person determining a signing tool or process' suitability under this Policy:

Russ Savage
Phone number: 602.542.2022
E-mail address: pa@mail.sosaz.com

3 General Provisions

3.1 Obligations

3.1.1 Signing community creation and management obligations

The ESI's Signers and Relying Parties constitute the signing community. They must establish contractual agreement on controls over the application and enrollment process, the identification and authentication process, the electronic signing tool and process, method of verifying the signature and the record integrity, and for ensuring that all aspects of the services, methods, operations and infrastructure related to signing tools and processes used under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

These contractual agreements shall operate in accordance with this Electronic Signing Policy and the laws of Arizona when fulfilling these obligations. The parties shall ensure that any LRAs operating on their behalf will comply with the relevant provisions of this Policy concerning the operation of LRAs. The parties will individually take all reasonable measures to ensure that Signers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of

hardware and software used within the ESI by any Signer, Relying Party or electronic records management provider.

3.1.2 Registration Authorities (RA)

The ESI parties (Signer and Relying Party) are responsible for performing all identification and authentication functions and all signing tool manufacturing and issuing functions. However, they may delegate performance of some or all of these obligations to an identified Registration Authority (RA) and/or Signature Dynamic Tools Provider (SDTP) provided they assume primary responsibility for third party service performance and assures performance consistent with this Policy.

3.1.3 LRA obligations (LRA duties)

Should the ESI allow the use of LRAs, then the parties must ensure that LRAs comply with all the relevant provisions of this Electronic Signing Policy. Administrators must be individually accountable for actions performed on behalf of the parties. (There must be evidence that attributes an action to the person performing the action for it to be individually accountable.) Records of all actions carried out in performance of LRA duties must identify the individual who performed the particular duty.

3.1.4 Representations By Signature Dynamic Tools Provider

The ESI's Signers and Relying Parties must establish a contractual agreement with the party or parties known as Signature Dynamic Tools Provider such that, for any tools issued or provided for use under this Policy, the Signature Dynamic Tools Provider certifies to the Signer, and to all Qualified Relying Parties who reasonably and in good faith rely on the Signature Dynamic Toolset that it has been issued in accordance with this Policy

3.1.5 Signer Obligations

A Signature Dynamic signing process results in an electronic signature by using the familiar physical elements of signing with pen and ink. The Signer needs to understand and accept that the same legal rights and obligations occur with the resulting electronic signature as with a physical ink to paper signature. Prior to signing, the Signer needs to be satisfied the document and signature are completed and bound in such a way that any change is detectable and that the signature is verifiable.

3.1.6 Relying Party Obligations

A Signature Dynamic signing process results in an electronic signature by using the familiar physical elements of signing with pen and ink. The Relying Party needs to understand and accept that the same legal rights and obligations occur with the resulting electronic signature as with a physical ink to paper signature. Prior to accepting the signed record, the Relying Party needs to be satisfied the document and signature are completed and bound in such a way that any change is detectable and that the signature is verifiable.

3.1.7 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy and its administration.

3.2 Requirements

An RA will ensure that its practices and actions are in accordance this Electronic Signing Policy.

A Signature Dynamic Tools Provider will ensure that its practices and actions are in accordance this Electronic Signing Policy.

An Signed Electronic Record Management system manager will ensure that its practices and actions are in accordance this Electronic Signing Policy.

3.3 Disclaimers of warranties and obligations

The State of Arizona assumes no liability whatsoever in relation to the use of AESI Signature Dynamic Tools for any use other than in accordance with this Electronic Signing Policy and any other explicit agreements.

The State of Arizona, its employees and agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this Electronic Signing Policy or in any other official document.

3.4 Liability

Except as expressly provided in this Policy and in ESI agreements, every Signature Dynamic Tools Provider, RA and Signed Electronic Record Management system manager is responsible to Qualified Relying Parties for direct damages suffered by such Relying Parties that are caused by the failure of the Signature Dynamic Tools Provider, RA or Signed Electronic Record Management system manager to comply with the terms of this Policy, and sustained by such Relying Parties as a result of reliance on a signature in accordance with this Policy, but only to the extent that the damages result from the use of Signature Dynamic Tools for a suitable applications listed as defined in this Electronic Signing Policy.

Except as expressly provided in this Policy and in ESI agreements, any Signature Dynamic Tools Provider, RA or Signed Electronic Record Management system manager disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

3.5 Interpretation & Enforcement

3.5.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the State of Arizona and the United States of America.

3.5.2 Severability, survival, merger, notice - Signature Dynamic Tools Provider[5]

Any Signature Dynamic Tools Provider, or agent of a Signature Dynamic Tools Provider, shall ensure that any of its agreements will have appropriate provisions governing severability, survival, merger or notice.

Any Signature Dynamic Tools Provider or agent of a Signature Dynamic Tools Provider shall have PA approval of its provisions governing severability, survival, merger or notice before beginning operation within an ESI and shall gain approval of any amendment to those provisions before such amendment can take effect.

3.5.3 Dispute Resolution Procedures

Each party shall ensure that any agreement they enter into provides appropriate dispute resolution procedures

3.6 Fees

No party may impose any fees on the reading of this Policy.

3.7 Publication & Repositories

3.7.1 Validation of Signature

Each Signature Dynamic Tools Provider (or a Signed Electronic Record Management system manager acting as agent for a Signature Dynamic Tools Provider) shall have a mechanism for appropriate Qualified Relying Parties to evaluate and validate a Signature Dynamics electronic signature.

3.8 Compliance Audit

The Policy Authority may outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the State of Arizona.

As deemed necessary by the PA, any Signing Tool Provider, Registration Authority, or Signed Electronic Records Management Provider may be required to submit to a compliance audit by an independent, nationally recognized security audit firm approved by the Policy Authority as being qualified to perform such an audit and as having significant experience in the application of Signature Dynamic electronic signatures and supportive cryptographic technologies. The purpose of such audit shall be to verify that the party and its delegated parties have a system in place to assure:

- the quality of the services provided,
- that the party complies with all of the requirements of this Policy, and
- the requirements of this Policy and any related agreement with the PA are complied with.

[5] An ongoing issue with any electronic signing process is assuring that the signed electronic record can be verified by any legally interested party throughout the legal life of the record. This provision is vague to allow for specific requirements to be developed for specific signing processes and the tools for them.

3.9 Intellectual property rights

No stipulation.

4 Identification And Authentication

4.1 Initial Registration

Registration of a Signer is typically done in the same fashion as that of a physical signature with ink and paper. Prospective signers often complete information in the document that identifies them. Prospective signers may be asked to provide forms of identification to the person before whom they make application for a Signature Dynamics electronic signature.

4.1.1 Authentication of Organization

No stipulation. Each community determines criteria for authentication of a participating organization.

4.1.2 Authentication of Individual -- No Affiliation

4.1.2.1 Identification & Authentication

No Stipulation. However, if an RA is required, the RA (or LRA) will require proof of identity as defined in the following section *Satisfactory Evidence of Identity* in authenticating the unaffiliated individual applicant.

4.1.3 Authentication of Individual – Affiliated

4.1.3.1 Identification & Authentication

No Stipulation. However, if an RA is required, the RA (or LRA) The Responsible Party shall require proof of identity as defined in the following section *Satisfactory Evidence of Identity*.

4.2 Satisfactory Evidence of Identity

The nature of satisfactory evidence of identity is determined by the certificate level of trust desired (See 2.4.8 Electronic Signature Framework of Trust).

5 Operational Requirements

5.1 Definitions

5.1.1 "Expert"

is a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert.

5.1.2 "Handwriting Measurements"

means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

5.1.3 "Signature Digest"
is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

5.1.4 "Signature Dynamics"
means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

5.2 Arizona §41-132 requires that a electronic signature be 'unique to the person using it.'
A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

- the signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and
- the signature digest is cryptographically bound to the handwriting measurements, and
- after the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

5.3 Arizona §41-132 requires that an electronic signature be capable of verification.
A signature digest produced by signature dynamics technology is capable of verification if:

- the acceptor of the electronically signed message obtains the handwriting measurements for purposes of comparison, and
- the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.

5.4 Arizona §41-132 requires that an electronic signature remain 'under the sole control of the person using it'.
A signature digest is under the sole control of the person using it if:

- the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and
- the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

5.5 Arizona §41-132 requires that a signature and the message be linked such that a change in the message invalidates the signature
The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

5.6 Application for a cross-certificate
When pertinent, the PA will identify cross-certificate (reciprocity) application procedures.

An application for a cross-certificate (reciprocity) does not oblige the PA to authorize a cross-certificate. The PA shall review any ESI's request for cross-certification and approve or deny any such request according to established procedures.

5.7 Computer Security Audit Procedures

All significant security events on the Signed Electronic Record Management system should be automatically recorded in audit trail files. The audit log shall be processed at least once a week. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived according to the PA's record retention schedule.

5.8 Records Archival

5.8.1 Types Of Records Archived

All relevant computer security audit data (including access logs) and files must be archived by or on behalf of the Relying Party.

5.8.2 Retention Period For Archive

Archive of the signing process information must be retained for the "legal" life of the most enduring document signed within the ESI. If that "legal" life is unknown, then for at least 30 years. Audit trail log file archives must be retained for at least six (6) months.

Any signed document may also have public records retention requirements that must also be met.

5.8.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must meet or exceed State of Arizona and Agency electronic records retention requirements for such material.

5.8.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a [short period of time] twenty four hours (or some specific period).

5.8.5 Archive Collection System (Internal Or External)

No stipulation.

5.8.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives.

5.9 Compromise And Disaster Recovery

5.9.1 Disaster Recovery Plan

The Signed Electronic Record Management system manager must have a disaster recovery and business resumption plan. The plan must set up and render operational a back-up facility at a location geographically removed from the primary operating location capable of providing Signed Electronic Record Management Services in accordance with

this Policy within forty eight (48) hours of an unanticipated emergency. The disaster recover and business resumption plan shall include a complete and periodic back-up facility readiness test. The plan shall include all appropriate documentation and be readily available to Qualified Relying Parties for inspection.

5.10 Signed Electronic Record Management system manager Termination

In the event that the Signed Electronic Record Management system manager ceases operation, all Signers, sponsoring organizations, RAs, Signature Dynamic Tools Providers, and Qualified Relying Parties will be promptly notified.. In addition, all parties with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All current and archived Signed Electronic Record Management system manager identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to the PA (or designate) within 24 hours of Signed Electronic Record Management system manager cessation and in accordance with this Policy. Transferred data shall not include any non-AESI data.

6 Physical, Procedural And Personnel Security

6.1 Physical Controls

6.1.1 Physical Security -- Access Controls

The Signed Electronic Record Management system manager, all RAs and all Signature Dynamic Tools Providers, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Signed Electronic Record Management system manager Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section on Procedural Controls (6.2.1). Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

6.2 Procedural Controls

6.2.1 Signature Dynamic Tools Provider Trusted Roles

All employees, contractors, and consultants of Signature Dynamic Tools Provider (collectively "Signature Dynamic Tools Provider personnel") that have access to or control over cryptographic operations that may materially affect the Signature Dynamic Tools Provider's issuance, use, suspension, or revocation of certificates shall, for purposes of this Policy, be considered as serving in a trusted role. Such Signature Dynamic Tools Provider personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the Signature Dynamic Tools Provider's operations.

6.2.2 Signed Electronic Record Management system manager Trusted Roles

All employees, contractors, and consultants of Signed Electronic Record Management system manager (collectively "Signed Electronic Record Management system manager personnel") that have access to or control over cryptographic operations that may materially affect the Signed Electronic Record Management system manager's use, suspension, or revocation of certificates, including access to restricted operations of the Signed Electronic Record Management system manager's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such Signed Electronic Record Management system manager personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the Signed Electronic Record Management system manager's operations.

6.2.3 Multiple Roles (Number Of Persons Required Per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a Signed Electronic Record Management system manager or Signature Dynamic Tools Provider server should be shared by multiple roles and individuals. Each account on the Signed Electronic Record Management system manager or Signature Dynamic Tools Provider server shall have limited capabilities commensurate with the role of the account holder.

6.3 Personal Security Controls

6.3.1 Background And Qualifications

Signed Electronic Record Management system managers, RAs, and Signature Dynamic Tools Providers shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

6.3.2 Signed Electronic Record Management system manager Background Investigation

Signed Electronic Record Management system managers shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and Signed Electronic Record Management system manager’s personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

6.3.3 Signature Dynamic Tools Provider Background Investigation

Signature Dynamic Tools Providers shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and Signature Dynamic Tools Provider’s personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

6.3.4 Training Requirements

All Signed Electronic Record Management system manager, RA, and Signature Dynamic Tools Provider personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

6.3.5 Documentation Supplied To Personnel

All Signed Electronic Record Management system manager, RA, and Signature Dynamic Tools Provider personnel must receive and read comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

7 Technical Security Controls

7.1 Signature Dynamics Signing Tool

No general stipulation. There are different biometrics based signature dynamics technologies used, security controls will be specific to the technology.

8 Policy Administration

8.1 Policy Change Procedures

8.1.1 List Of Items

Notice of all proposed changes to this Policy under consideration by the Policy Authority that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to the designated contact for the ESI, and will be posted on the World Wide Web site of the Policy Authority. CRs shall post notice of such proposed changes in their repositories and shall advise their Signers, in writing or by e-mail, of such proposed changes.

8.1.2 Comment Period

Impacted users may file comments with the Policy Authority within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 Publication & Notification Procedures

A copy of this Policy is available in electronic form on the Internet at http:www.sos.state.az.us/pa, and via e-mail from pa@sos.state.az.us.

CRs shall post copies of this Policy in their repositories.

8.2.1.1 Notification mechanism

The PA will notify, in writing, all CRs that are directly cross-certified with the AESI of any proposed changes to this Electronic Signing Policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed

effective date of change. The PA may request CRs to notify their Signers of the proposed changes.

8.2.1.2 Mechanism to handle comments

Written and signed comments on proposed changes must be directed to the PA. Decisions with respect to the proposed changes are at the sole discretion of the PA.

8.2.2 Items whose change requires a new policy

If a policy change is determined by the PA to warrant the issuance of a new policy, the PA may assign a new Object Identifier (OID) for the modified policy.